

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
One grey/black iPhone, currently located at the  
FBI, 600 Arch Street, Philadelphia, PA, 19106

Case No. 19-1323-M

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

One grey/black iPhone, currently located at the FBI, 600 Arch Street, Philadelphia, further described in Attachment A

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

Evidence, contraband, fruits and instrumentalities of a crime, further described in Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 USC 2422(b)  
18 USC 2251  
18 USC 2252

Offense Description  
online enticement of a minor, production of child pornography, possession of child pornography

The application is based on these facts:  
See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

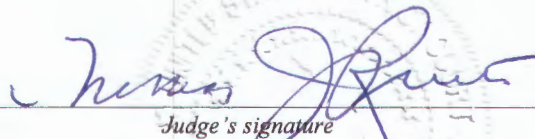
  
Applicant's signature

FBI SA Daniel Johns  
Printed name and title

Sworn to before me and signed in my presence.

Date: 8-2-19

City and state: Philadelphia, PA

  
Judge's signature

Hon. Thomas J. Rueter, U.S. Magistrate Judge  
Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Daniel J. Johns, a Special Agent (SA) with the Federal Bureau of Investigation, Philadelphia Division, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of FBI for 12 years, and am currently assigned to the Violent Crimes Against Children Squad.
2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
3. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause.
4. This affidavit is presented in support of an application for a search warrant for an grey/black iPhone located at FBI Philadelphia Division, 600 Arch Street, Philadelphia, PA 19106, further described in Attachment A, for evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Section 2422(b) (online enticement of a minor), Section 2251 (production of child pornography), and Section 2252(a)(4)(B) (possession of child pornography), further described in Attachment B.
5. In summary, the following facts establish that there is probable cause to believe that CHRISTOPHER O'SULLIVAN, who resides at 5130 Springfield Avenue, Unit 2, Philadelphia, PA 19143, attempted to produce child pornography, and persuaded, induced, enticed

and/or coerced a child to engage in sexually explicit conduct, using a device that was found on his person on August 1, 2019.

### **LEGAL AUTHORITY**

7. 18 U.S.C. § 2422(b) prohibits a person from knowingly persuading, inducing, enticing or coercing a minor to engage in any sexual activity for which any person can be charged with a criminal offense, or attempting to do so.

8. 18 U.S.C. § 2251 prohibits a person from employing, using, persuading, inducing, enticing or coercion a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct, where the person knows that such visual depiction will be transmitted using any means or facility of interstate or foreign commerce, or if the visual depiction is produced using materials that were transported in or affecting interstate or foreign commerce, by any means, including by computer, or attempting to do so.

9. 18 U.S.C. § 2252(a)(4)(B) prohibits a person from possessing any visual depiction that has been transported using any means or facility of interstate or foreign commerce, or that was produced using material that were mailed, transported or shipped in interstate or foreign commerce.

### **DEFINITIONS**

10. The following definitions apply to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see Title 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (See Title 18 U.S.C. § 2256(5)).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. (See Title 18 U.S.C. § 2256(2)). An image can depict the lascivious exhibition of the genitals or pubic area even if the child is clothed, *see United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), *cert. denied*, 513 U.S. 1109 (1995); *United States v. Caillier*, 442 F. App'x 904 (5th Cir. 2011), so long as it is sufficiently sexually suggestive under the factors outlined in *United States v. Dost*, 636 F. Supp. 828 (S.D. Cal. 1986), *aff'd sub nom, United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *aff'd*, 813 F.2d 1231 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987).

e. "Computer," as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Minor" means any person under the age of eighteen years. (See Title 18 U.S.C. § 2256(1)).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and co location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e mail address," an e mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded

and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. (See Title 18 U.S.C. § 2510(15)).

j. "Hash Value" is a mathematical value generated by applying an algorithm to a computer file that is represented by a sequence of hexadecimal digits. Among computer forensics professionals, a hash value is generally considered to be a unique signature or fingerprint for a file.

**BACKGROUND REGARDING COMPUTER/ELECTRONIC DEVICES  
AND THE INTERNET**

11. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce

the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Cell phones and more advanced devices known as "smart phones" function the same as computers and can run computer software and applications, create and edit files, go on the Internet, chat, text, email, and interact with others on the Internet, and store, send, and receive files, among other functions. Cell phones and smart phones have been used by child pornographers to send, receive, store, and produce images depicting child pornography, as well as engage in voice, email, text, and real time chat conversations with minors and others. Cell phones and smart phones can contain SD cards and/or SIM cards that can store data such as pictures, videos, text messages, contact lists, call logs and other data.

d. GPS, or Global Positioning System, devices can be portable devices used to obtain directions to destinations or show roads and directions in a given area. GPS devices can store the route an individual traveled. GPS devices have been used by individuals to obtain directions when they travel to meet a minor for sexual purposes.

e. Child pornographers can convert photographs into a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

f. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

h. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals

such as Google, Yahoo!, Hotmail, Sky Drive or One Drive, and Dropbox among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or device, such as a cell phone or "smart phone", with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer devices in most cases.

i. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

#### **CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTOR**

12. I know from my training and experience that the following characteristics are prevalent among individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography may collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals may also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their sexual fantasies involving children.

c. The majority of individuals who collect child pornography may often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography may maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often may collect, read, copy or maintain names, addresses (including e-mail addresses), phone

numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

f. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. However, some individuals may dispose of their collection of their sexually explicit materials or only seek them out when they want to view them in order to conceal their activities for fear of being caught.

#### **BACKGROUND OF THE INVESTIGATION**

13. On July 23, 2019, the parents of a twelve-year-old minor victim (hereinafter referred to as "VIC"), made a complaint at a Philadelphia middle school. The parents, school and VIC are known to law enforcement. The parents provided school officials with VIC's cellular phone, which contained several hundred text messages through Apple's iMessage service. These messages were between VIC and 610-513-1564. VIC had this number saved in his phone as "Mr O." The messages appeared to be sexual in nature and school officials advised VIC's parents to file a complaint with the Philadelphia Police Department (PPD). Prior to doing so, school officials created a video file which captured the messages between VIC and O'SULLIVAN. Additionally, an Information Technology employee who is known to law enforcement utilized software to back-up the messages on VIC's cellular phone. Both of these files have been provided to law enforcement.

14. VIC's parents filed a complaint with the PPD and brought VIC in for an interview. VIC told PPD that he had communicated with Mr. SULLIVAN, whom he identified by photograph. The photograph identified by VIC depicted CHRISTOPHER D. O'SULLIVAN, date of birth 8/xx/1988, home address 5130 Springfield Avenue, Unit 2, Philadelphia, PA 19143. VIC told police that he never sent O'SULLIVAN naked images, nor had O'SULLIVAN touched him inappropriately. VIC stated that he had sent O'SULLIVAN an image of himself without a shirt and that O'SULLIVAN had asked him if he spoke to his friends about masturbation.

15. On July 31, 2019 your affiant reviewed VIC's cellular phone, which contained hundreds of messages from O'SULLIVAN. In those messages, O'SULLIVAN and VIC discussed out-of-state excursions, which included hiking and camping, as well as video games and general conversation. VIC's messages were primarily in response to inquiries by O'SULLIVAN and were very brief. The brevity of VIC appeared to annoy O'SULLIVAN, in response to which he made several comments. For example, O'SULLIVAN sent the following messages to VIC: "Yo man, i know you're busy with camp and stuff but message me when you get the chance. I feel like your annoyed with me or something," "Alright but how come you haven't gotten back to me all day?," and, "Let's see if you do a better job messaging me now. I know you're tired. And maybe your phone is low. But if you're up in a bit i'll be waiting to hear from ya. I wanna see if you're all talk or actually a man of your word this time."

16. O'SULLIVAN also sent various messages that were suggestive. These included messages on June 30, 2019 wherein he asked VIC, "Can i still help you get better/more confident." VIC responded affirmatively, and O'SULLIVAN then said, "And what's something you can help me get better at?" This was followed by O'SULLIVAN messaging, "Id say video

games.. but idk if i really wanna get better has," and "Huh?" On July 4, 2019, O'SULLIVAN also requested VIC delete their messages. For example, he stated, "I hope you made sure our other messages were closed/gone."

17. On July 4, 2019, O'SULLIVAN sent an image to VIC that contained what appeared to be a gift card with a code on the back. Based upon my training and experience, gift cards can be utilized to make online purchases as long as the code for the gift card is provided. After providing the gift card to VIC, O'SULLIVAN stated, "Don't leave me hanging any more bruh And you still gotta snap me back." Based upon my training and experience, "Snap" is a reference to Snapchat, a popular messaging and social media services wherein users can exchange text, image and video messages, apply filters to image and video messages, and post publicly on social media feeds. Snapchat messages can be designed to destruct within seconds, hours or a day. For this reason, Snapchat is often thought to be a safe mechanism to exchange naked images. Additionally, Snapchat is commonly used by persons enticing minors due to the perceived security of deleted messages. Based upon my training and experience, when an adult communicates with a child primarily through an SMS type service, like iMessage, but requests other images sent via Snapchat, it is because they do not want any record of the messages having been sent.

18. O'SULLIVAN appeared to have utilized Snapchat to exchange images that were sexual in nature with VIC, based upon various references, including but not limited to a message sent on July 6, 2019, wherein O'SULLIVAN asked VIC to look at the "snaps" he sent VIC, and told VIC not to worry because they were all "pg." Additionally on July 13, 2019, O'SULLIVAN asked VIC to "just send me snaps of what you're doing or where you are.. not the

other stuff." On July 18, 2019, O'SULLIVAN asked VIC why he had not viewed the snaps O'SULLIVAN sent. Later that same day, O'SULLIVAN sent the following messages to VIC: "Glad you finally snapped me back 🖐️" and "You can send me regular pics too. I like both." Lastly on July 19, 2019 at 1:17 a.m., O'SULLIVAN asked VIC to "Send me some good ones buddy." On July 19, 2019 at 12:18 p.m., O'SULLIVAN sent VIC a message stating "Hey." VIC responded at 12:18 p.m., stating "Hey," then VIC wrote, "I did now," at 12:19 p.m. I know from reviewing VIC's phone that on July 19, 2019, at 12:19 p.m. VIC's phone was utilized to take a picture of a penis. Based upon my training and experience, the penis depicted in the image was of a prepubescent male of the same race as VIC. Additionally, the angle of the image appears to indicate that the individual holding the cellular phone took the picture of himself. O'SULLIVAN responded to VIC at 12:20 p.m., "Nicee." VIC responded at 12:24 p.m., "yeah." O'SULLIVAN then requested of VIC, "If you're okay with it you should try and send me a nice sexy video 😊 haha," followed by, "And obviously you don't have to." Later that same day at 3:16 p.m., O'SULLIVAN sent VIC another gift card, then sent the following messages: "Hey i want you to have this, but i also want you to keep messaging me while im traveling please 😊," followed by, "And send me a video?"

19. On July 9, 2019, O'SULLIVAN and VIC had the following exchange:

OS: Would you want me to pick you up a little before everyone else to do stuff for a little then?

Or are you thinking you don't want to today?

VIC: Not today to. Tommorow

OS: we'll be heading out for camping tomorrow

VIC: yea we can do it then

OS: Why do i have a feeling you're not gonna want to then either?

VIC: No. I'm am it batter. There. At the camp

OS: Yeah be it seems like you say you're interested and then change your mind and say not today. Which is totally okay.. i just wanna make sure it's something you actually WANT to do

VIC: It is. I like it. It feels good

OS: I agree.. so definitely tomorrow? You'll even take the lead?

OS: And you sure you don't think we can do any today?

VIC: Ok

OS: Can you at least send me some snaps this morning then?

OS: ??

OS: Also did you wanna try and make a copy of your key today?

20. This conversation was followed up on July 11, 2019, when O'SULLIVAN and VIC had the following exchange:

OS: Let's see if you do a better job messaging me now. I know you're tired. And maybe your phone is low. But if you're up in a bit i'll be waiting to hear from ya. I wanna see if you're all talk or actually a man of your word this time.

VIC: Ok

OS: And you already know how i feel about these short behind responses ☐♂

VIC: Yeah that how i text

OS: Sometimes it's fine.. like if im asking a basic question that deserves a basic response.. but other times it just comes off like you don't got time for me

VIC: Ok I will text you when I'm done a nap

OS: Thanks bud. Once you look through the photos and stuff tell me your top pics. Hey Haj. And remember im only giving one of these cards if you message better

21. On July 20, 2019, O'SULLIVAN asked VIC if he ever talked to his friends about "jerkin off?" Based upon my training and experience "jerkin off" means masturbation.

20. Your affiant spoke to Vicki Humphreys, a private investigator, who was retained by the attorney for the middle school, O'SULLIVAN's employer. Humphreys provided contact information for O'SULLIVAN, which was provided to her by the school. The address provided was 5130 Springfield Avenue, Unit 2, Philadelphia, PA 19143. Additionally, the school provided the cellular phone number for O'SULLIVAN, via legal counsel, as 610-xxx-1564. Legal counsel for the school confirmed that this cellular number was provided by O'SULLIVAN to the school.

21. On July 31, 2019 physical surveillance was conducted at 5130 Springfield Avenue, Unit 2, Philadelphia, PA 19143. No vehicles registered to O'SULLIVAN were located.

22. On August 1, 2019 a federal search warrant signed by the Honorable Thomas J. Rueter, United States Magistrate Judge, was executed at 5130 Springfield Avenue, Unit 2, Philadelphia, PA 19143. At the time of the search warrant execution, O'SULLIVAN was not present. During the search, O'SULLIVAN arrived and was allowed to enter the residence. On O'SULLIVAN's person was a black/grey Apple iPhone. O'SULLIVAN was provided with his *Miranda* warning by your affiant, after which he provided the PIN to his cellular phone. Your affiant utilized the PIN to place the phone into airplane mode.

23. In messages with VIC, O'SULLIVAN sent images with metadata identifying his phone as an iPhone Xr. The phone in your affiant's possession appears to be an iPhone Xr.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER/PHONE SYSTEMS**

24. Searches and seizures of evidence from computer devices, cell phones, smart phones, and GPS's commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, cell phones, smart phones, GPS's, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer and electronic systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should

analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

25. In addition, there is probable cause to believe that these computer and electronic devices are all instrumentalities of the crimes, and should all be searched and seized as such.

#### **SEARCH METHODOLOGY TO BE EMPLOYED**

26. To search for electronic data contained in computer, phone, or electronic device hardware, computer, phone, or electronic device software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. searching for image files to locate images of children engaging in sexually explicit conduct, examining log files associated with the receipt, transmission, and viewing of such images, and examining all of the data contained in such computer hardware, computer software, and /or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. surveying various file directories and the individual files they contain;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B;

g. searching for malware in order to evaluate defenses, such as viruses;  
and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

#### **ABILITY TO RETRIEVE DELETED FILES**

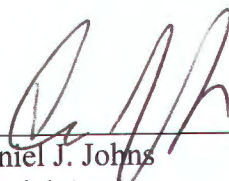
27. Computer files or remnants of such files on traditional or conventional mechanical computer hard drives can typically be recovered months or even years after they have been downloaded onto the hard drive, deleted or viewed via the Internet. Electronic files downloaded to the hard drive or storage device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily

available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from these conventional types of hard drives depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

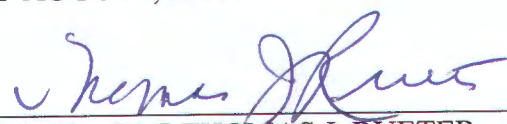
28. Other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory based hard drives and devices. This technology has been traditionally used for small thumb drives where files and data are stored electronically, but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSD's and also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and overwritten. Because of how these flash, memory-based drives function it may limit how much data, if any, can be recovered from these types of devices.

**CONCLUSION**

29. Based upon the information above, I respectfully submit that there is probable cause to believe that violations of Title 18 U.S.C. Sections 2422(b) (online enticement of a minor), 2251 (production of child pornography), and 2252(a)(4)(B) (possession of child pornography) have been committed, and that evidence, contraband, fruits and instrumentalities of those violations, further described in Attachment B, is located on the black/grey iPhone in your affiant's possession, further described in Attachment A. Therefore, I respectfully request that the attached warrant be issued for the device in Attachment A, authorizing the search and seizure of the items listed in Attachment B.

  
\_\_\_\_\_  
Daniel J. Johns  
Special Agent  
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED  
BEFORE ME THIS 2nd DAY  
OF AUGUST, 2019.

  
\_\_\_\_\_  
HONORABLE THOMAS J. RUETER  
United States Magistrate Judge



**ATTACHMENT A**

**Location to be Searched**

**Black/Grey iPhone currently located at the  
FBI Philadelphia Division, 600 Arch Street, Philadelphia, PA 19106**



**ATTACHMENT B**  
**ITEMS TO BE SEARCHED FOR AND SEIZED**

Evidence of violations of 18 U.S.C. 2422(b), 2251, and 2252, including the following:

1. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct, including those in opened or unopened e-mails or text messages. These include both originals and copies.

2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, Internet history, photographs, and any other electronic data or other memory features contained in the devices, smart phones, cell phones, computers, or SIM cards including correspondence, records, opened or unopened e-mails, text messages, chat logs, and Internet history, pertaining to the production, possession, receipt, access to or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed.

3. All communications and files with or about potential minors involving sexual topics or in an effort to seduce the minor or efforts to meet a minor.

4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

5. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

6. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.

7. Documents and records regarding the ownership and/or possession of the searched items.

8. During the course of the search, photographs of the devices may also be taken to record the condition thereof and/or the location of items therein.

9. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

10. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any visual depictions described in paragraph 1 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.

The above seizure of computer, electronic device, and computer-related hardware relates to such computer-related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting.